REMARKS

Please reconsider the claims in the application in view of the remarks below.

Claim Rejection – 35 U.S.C. §103(a)

The Office Action rejected claims 1, 2, 12-15, 25, 26 and 33 under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent No. 6,405,315 ("Burns") in view of U.S. Patent No. 6,959,384 ("Serret-Avila"). The Office Action rejected claims 3, 7-8, 10, 11, 20, 21, 23, 24, 27, 29-32 under 35 U.S.C. §103(a) as allegedly being unpatentable over Burns in view of Serret-Avila and further in view of U.S. Patent No. 6,931,543 ("Pang"), in view of U.S. Patent No 5,124,117 ("Tatebayashi"). Claims 4, 17 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Burns and Serret-Avila in view of U.S. Patent No. 5,608,801 ("Aiello"). Of the pending claims, claims 1, 14, 25 and 33 are independent.

The Office Action maintained the same previous rejections of the claims. In responding to the applicants' previous arguments that Burns and Serret-Avila do not disclose or suggest storing integrity tree data structure at the client, the Examiner further responds that, "while the hash is stored with the data at the storage device, the client also stores the generated hash of the data while the data object is being created. The storage device has absolutely no encryption capabilities. Therefore, the data is hashed and encrypted by the client, which requires storage, prior to being sent to the storage device," citing Burns, Col. 3, lines 19-21 and Col. 3, lines 16-19.

To further clarify what is being claimed, independent claims 1, 14, 25 and 33 are being amended to additionally recite, "wherein said root data structure is not written out to the storage

device." Support for the amendment can be found at least in paragraphs [0016] and [0017], and Figure 4. The disclosure therein explicitly describe testing for root of the integrity tree when writing each data block, and when it is determined that the root of the integrity tree is reached, completing the process, without writing to the storage utility. Thus, the root of the integrity tree is never written out to the storage utility, and only the client keeps it locally.

Burns on the other hand stores its data objects and hash values on a network storage device. Regardless of whether Burns' storage device has no encryption capabilities, it remains that Burns stores hash values at the storage utility. In Burns, client first finds the encrypted hash stored on the network storage device for integrity checking of the chunk (See, Burns, Col. 8, lines 5-14 and Col 10, line 60 – Col. 11, line 17).

In the present application, the root of the integrity tree is stored on the client ("customer") computer that uses the storage utility. An integrity check of data retrieved from the network storage utility is performed by using the "stored integrity value" stored on the client. The client does not go to the storage utility to find the integrity value. Burns, alone or in combination with other cited references, does not disclose or suggest, at least this element. Furthermore Serret-Avila and all of the other cited reference do not make up for that deficiency.

For at least the above reason, applicants believe that independent claims 1, 14, 25 and 33, and their respective dependent claims at least by virtue of their dependency are not obvious over Burns and Serret-Avila.

With respect to the dependent claims rejected also in view of the rest of the references, because those references fail to disclose or suggest what Burns and Serret-Avila lack as explained above with respect to independent claims, those dependent claims also are believed to be unobvious over the cited references.

In addition, with specific reference to the rejection of claim 11, the Examiner errs in alleging Burns in Col. 5, lines 40-45 discloses, "comparing integrity of data blocks to be read on a path from said root data structure via successive higher meta-data blocks and meta-data block layers until a desired data block at a first layer is read." That passage of Burns refers to a client wanting to update a network object reads the data, decrypts, updates and encrypts the data. Burns, however, does not disclose or suggest comparing the integrity of data blocks to be read on a path from said root data structure via successive layers. Further, none of the applied references used to reject claim 11, i.e., Serret-Avila, Pang, and Tatebayashi make up for what Burns lacks in that respect. Therefore, claim 11 is unobvious over the cited references for at least this additional reason.

On page 2 of the Office Action, the Examiner further alleges that applicants argue against the references individually. Contrarily, applicants are not arguing against the references individually; rather in pointing out the specific sections of specific references, applicants are countering the Examiner's position, which cites sections of those individual references. Applicants are arguing that those cited sections of the references individually or in combination do not disclose or suggest what the Examiner alleges.

In view of the foregoing, this application is now believed to be in condition for allowance, and a Notice of Allowance is respectfully requested. If the Examiner believes a telephone conference might expedite prosecution of this case, applicant respectfully requests that the Examiner call applicant's attorney at (516) 742-4343.

Respectfully submitted,

Eunhee Park
Registration No.: 42, 976

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza, Suite 300
Garden City, N.Y. 11530
(516) 742-4343